The Future of Smart Cards : Technology and Application

Vincent Cordonnier

Professor - University of Lille - France

RD2P - CHR CALMETTE

59037 LILLE Cedex

Chairman of the IFIP Special Group on Smart Cards

1 INTRODUCTION

For the twenty last years, the smart card market has grown from nothing to approximately a billion cards a year for 1996. Many applications have been identified as typical areas of that technology, mostly electronic money and identification of individuals. However, for many service providers and application designers, the smart card domain is still hazardous and not perfectly well identified in terms of technology and capabilities. The ratio of project failures is extremely high and many existing applications do not fit with their initial definition. This remark leads to give the greatest importance to the identification of that technology and its existing and potential characteristics and market. Then, it becomes easier to look at the future as the convergence between technological improvements and innovative applications requirements.

2 AN OVERVIEW OF THE SMART CARD STATUS

A smart card can be roughly identified as a portable, secure and intelligent memory. As a portable device it is almost always related to an individual and gives this individual access facilities to various services when moving around. Security is provided by both temper resistance and encryption of stored and exchanged data. Intelligence appears in both an efficient management of stored data and the capability to adapt the activity to the identified reader or terminal or external partner. Whatever can be the embarked application, a card usually behaves as a passive component. It just has to react to questions, commands or access requirements which are delivered by the terminal.

From the technological point of view, a card is composed of a data memory, a control unit which can either be a logical circuit or a microprocessor. In that case, the program to be executed is permanently stored in a ROM memory and cannot be altered. Two other components, the input-output module and the physical security module must be added to realise a complete device.

Typical characteristics are 1 to 8 kilobytes for the data memory, 1 to 16 kilobytes for

the ROM memory, 9,600 bits per second for the serial communication link and a 8 bit microprocessor with a 4 MHz clock provided by the terminal. These limits will not grow faster than the average silicon improvement for the five next years.

From the application point of view, the success has led to an impressive number of services covering the international level (credit cards) and the local level (cities, companies, universities). In every case, a card can be seen as a replacement tool for various portable devices such as identity papers, purses, portable data files. It is more reliable, more secure and can support automatic exchanges with the service provider.

3 THE FUTURE OF TECHNOLOGY

There are many possible tracks for improving the flexibility and intelligence of smart cards. They will appear at the component level, the software level and the functional level. Then many innovative applications will be made possible. Actually, it seems more logical to first look at the requirements of these possible new applications and then to design smart cards of the future. As for many other technologies, the final result will probably be issued from a convergence of these two complementary approaches.

3.1 The component level

As the surface of the chip is restricted to 25 mm², most of the improvements will not result from drastically increasing the number of gates. For the microprocessor itself, a RISC approach will probably offer a better ratio between performances, complexity and electrical consumption. Some manufacturers prepare a 32 bits approach (Cascade project). The resulting power will serve security for high level algorithms, protocols and biometrics. Another important issue is the communication link which will require higher rates and propose possibilities for contactless accesses. Eventually, it seems interesting to partly merge the ROM and the EPROM memories into a unique memory space. Dedicated hardware for fast encryption-decryption algorithms is another interesting issue.

3.2 The software level

So far smart cards manufacturers and application issuers have decided to write in a single ROM code, the application itself and the basic functions of the operating system. Such a software architecture is interesting because of security and memory space saving. As many people now think of multi application cards, it will become necessary to clearly separate these to layers.

Operating systems for smart cards will become a major issue for the next generation. Obviously, this operating system will be characterised by a few properties which are typical of the smart card working environment:

- A fixed and dedicated memory,
- A single communication link,
- A unique and simple file and data management,

- A high level of security against any possible fraud, and, for the most advanced
- Capability for multi application, multi services and multi users.

3.3 The functional level

As previously mentioned, smart cards are mostly considered as memories and the microprocessor is mostly used to bring the most secure and intelligent management of that memory including communication with external local or remote devices. The ultimate example of this memory management approach is the CQL card which works as a relational data base with a great flexibility. There are many ways to give a card more capabilities and to use the microprocessor and its operating system for other purposes.

Code importation looks like a promising track. Assuming that a limited memory space does not allow to store many programs, it becomes interesting to make the card capable of directly obtaining the program it must execute from the terminal. Code importation is the most promising approach for the universal card.

Active cards represent another innovative possibility. By processing an external request and its stored data, the card can produce a new information to be presented to the terminal. Such a function is an excellent mean to save privacy. Eventually, the active card will execute more processing to provide the convenient response regarding to its content, the status of the partner and the security level of the transaction.

Biometry, including expert system, will take place in smart cards. Because the presently used PIN number is known as not secure enough and easy to fraud, a better identification technology become mandatory. Prototypes which analyse the voice, recognise fingerprints or the shape of the hand already exist.

4 THE FUTURE OF APPLICATIONS

For many years, application designers hesitated between a centralised solution using a network to access a server and a decentralised one using distributed cards. Now, everybody agrees that networks and cards are totally complementary. Internet will certainly needs smart cards to authentify secured accesses as, for example to manage money transfers or to protect private communications; pay-tv channels needs smart cards to personalise an access. But, potentially, the most powerful network is the mobile telephone. Smart cards have been closely associated to GSM to support identification and auxiliary services. Smart card also use the GSM facilities to access many other applications. A key to the future is probably to look at the smart card as the natural extremity of any secured communication network.

5 CONCLUSION

The estimated production before the end of the century is more than four billion smart cards a year. The second generation is still to be designed and validated. Manufacturers and major application issuers will promote new technologies if and only if they bring a possibility to extend the market and to collect more and more transactions. Research on

smart cards will propose a lot of possible improvements. They will only be accepted if they offer a good balance between quality of services, flexibility and security.